We claim:

1. A method for Galois field ($GF(2^m)$) multiplication, where m is a positive integer, and the $GF(2^m)$ multiplication operation calculates the multiplication of two polynomials producing a product which is divided by a generator polynomial, and wherein the multiplication operation is further combined with the division operation whereby the $GF(2^m)$ multiplication may be computed in a single logic stage, the method comprising:

generating x^{m-i} polynomial coefficient terms from multiplication and division operations, where i is a variable;

combining like x^{m-i} polynomial coefficient terms from the multiplication and division operations; and

computing a recurrence relation using the combined x^{m-i} polynomial coefficient terms for the single $GF(2^m)$ multiplication function.

2. The method of claim 1 wherein the recurrence relation for a single $GF(2^m)$ multiplication function is $Y(i) = Y(i-1) + (q_{m-i}*p + Y(i-1)_{2m-1}*g)*x^{m-i}$, $i=1, 2, \ldots, m$ and where $Y(0) = 0$.

3. The method of claim 1 further comprising:

outputting results from computing the recurrence relation; and

storing the results in computer readable form.

4. A method for Galois field ($GF(2^m)$) multiplication, where m is a positive integer, and the $GF(2^m)$ multiplication operation calculates the multiplication of two polynomials producing a product which is divided by a generator polynomial, and wherein the multiplication

operation is further combined with the division operation whereby the $GF(2^m)$ multiplication may be computed in a single logic stage, the method comprising:

generating x^{m-i} polynomial coefficient terms from multiplication and division operations, where i is a variable;

combining like x^{m-i} polynomial coefficient terms from the multiplication and division operations; and

computing a simplified recurrence relation using the combined x^{m-i} polynomial coefficient terms for the single $GF(2^m)$ multiplication function thereby calculating m by m bits for the simplified $GF(2^m)$ multiplication function.

5. The method claim 4 wherein the simplified the recurrence relation for the single $GF(2^m)$ multiplication function is $Y(i) = Y(i-1) + (q_{m-i}*p + Y(i-1)_{m-1}*g)*x^{m-i}$, $i=1, 2, \ldots, m$ and where $Y(0) = 0$.

6. The method of claim 4 further comprising:

outputting results from computing the simplified recurrence relation; and

storing the results in computer readable form.

7. A GF multiplication circuit cell producing result $Y(i)_j$ for $i \in \{1, 2, \ldots, m\}$, $j \in \{0, 1, \ldots, m-1\}$, where m is a positive integer, and a selected i and j value comprising:

a bit q_{m-i} selected from the set $\{q_{m-1}, q_{m-2}, \ldots, q_{m-i}, \ldots, q_0\}$ of first product inputs;

a bit p_j selected from the set $\{p_{m-1}, p_{m-2}, \ldots, p_j, \ldots, p_0\}$ of second product inputs;

a bit g_j selected from the set $\{g_{m-1}, g_{m-2}, \ldots, g_j, \ldots, g_0\}$ of generator polynomial coefficients;

the most significant bit $Y(i-1)_{m-1}$ of the previous GF multiplication circuit cell values;

the value of the rightmost neighbor bit $Y(i-1)_{j-1}$ of a previous GF multiplication cell;

a logic device producing q_{m-i} AND p_j as output A;

a logic device producing $Y(i-1)_{m-1}$ AND g_j as output B; and

a logic device producing A XOR B XOR $Y(i-1)_{j-1}$ as output $Y(i)_j$.

8. The GF multiplication circuit cell of claim 7 disposed within an m-by-m array of GF multiplication circuit cells for producing a Galois Field (2^m) multiplication result Y, where m is a positive integer, further comprising:

input operand $q = (q_{m-1}\ q_{m-2}\ \ldots\ q_0)$;

input operand $p = (p_{m-1}\ p_{m-2}\ \ldots\ p_0)$;

input operand $g = (g_{m-1}\ g_{m-2}\ \ldots\ g_0)$;

the $Y(i-1)_{m-1}$ and the $Y(i-1)_{j-1}$ array border GF multiplication circuit cell input values set to 0;

output Y results; and

an m-by-m array of interconnected GF multiplication circuit cells.

9. The GF multiplication circuit cell of claim 8 wherein the m-by-m array of interconnected GF multiplication circuit cells further comprises:

the interconnections of the GF multiplication circuit cells governed by the equation

$Y(i) = Y(i-1) + (q_{m-i}*p + Y(i-1)_{m-1}*g)*x^{m-i}$, i=1, 2, …, m and where Y(0) = 0.

10. The GF multiplication circuit cell of claim 8 wherein the m-by-m array of GF multiplication circuit cells is further disposed within a grouping of multiple m-by-m arrays in a processor execution unit and further comprises:

a GF (2^m) multiplication instruction with a data type field specifying at least one GF (2^m) multiplication operation; and

means for connecting the multiple m-by-m arrays inputs and outputs for performing at least one GF (2^m) multiplication in the execution of the GF (2^m) multiplication instruction.

11. The GF multiplication circuit cell of claim 8 wherein the input operands q = (q_{m-1} q_{m-2} … q_0), p = (p_{m-1} p_{m-2} … p_0), and g = (g_{m-1} g_{m-2} … g_0) are connected to read outputs of at least one storage unit in a processor system.

12. The GF multiplication circuit cell of claim 8 wherein the output Y results are connected to at least one storage unit write inputs in a processor system.

13. The GF multiplication circuit cell of claim 11 wherein the at least one storage unit is a processor accessible register file.

14. The GF multiplication circuit cell of claim 12 wherein the at least one storage unit is a processor accessible register file.

15. An apparatus for computing a GF (2^m) multiplication, where m is a positive integer, the apparatus comprising:

means to calculate a portion of the GF (2^m) multiplication function in a GF multiplication circuit cell;

means to interconnect an m-by-m array of GF multiplication circuit cells;

means to connect a plurality of inputs to the m-by-m array; and

means for storing the results of the GF (2^m) multiplication.

16. A computer-readable medium whose contents cause a computer system to perform at least one GF multiplication, the computer system having a program storage unit where at least one GF multiplication instruction is stored and program execution means including at least one m-by-m array of GF multiplication circuit cells responsive to a GF multiplication instruction in an execution unit, by performing:

fetching the GF multiplication instruction from the program storage unit; and

executing the GF multiplication instruction whereby the computer system performs at least one GF (2^m) multiplication by the program execution means.

17. The computer-readable medium of claim 16 wherein the program execution means further comprises:

a plurality of processing elements (PEs);

means to distribute instructions fetched from the program storage unit to the PEs; and

each PE having at least one m-by-m array of GF multiplication circuit cells in an execution unit whereby more than one GF multiplication is accomplished in parallel.

18. A method for executing at least one GF multiplication instruction contained in a very long instruction word (VLIW) on a computer system having VLIW execution means including a VLIW storage unit and at least one m-by-m array of GF multiplication circuit cells responsive to a GF multiplication instruction in an execution unit, the method comprising:

fetching the VLIW from the VLIW storage unit; and

executing the VLIW including the GF multiplication instruction whereby the computer system performs at least one GF (2^m) multiplication by the VLIW execution means.

19. The method of claim 18 wherein the VLIW execution means further comprises:

a plurality of processing elements (PEs);

each PE having at least one m-by-m array of GF multiplication circuit cells in an execution unit; and

means to invoke a VLIW containing a GF multiplication instruction on each PE in parallel whereby more than one GF multiplication is accomplished in parallel.